(12) UK Patent Application (19) GB (11) 2 350 021 (13) A

(43) Date of A Publication 15.11.2000

(21) Application No 0004575.7

(22) Date of Filing 25.02.2000

(30) Priority Data
(31) 11049678 (32) 26.02.1999 (33) JP

(71) Applicant(s)
Rohm Co. Ltd
(Incorporated in Japan)
21 Saiin Mizosaki-cho, Ukyo-ku, Kyoto-shi, Kyoto 615, Japan

(72) Inventor(s)
Junichi Hikita
Haruo Taguchi
Yoshihiro Ikefuji

(74) Agent and/or Address for Service
Mewburn Ellis
York House, 23 Kingsway, LONDON, WC2B 6HP, United Kingdom

(51) INT CL[7]
H04L 9/32 // G07F 7/10

(52) UK CL (Edition R)
H4L LECCX

(56) Documents Cited
EP 0743622 A2 EP 0332117 A2 JP 100327142 A
US 6058477 A US 4734568 A

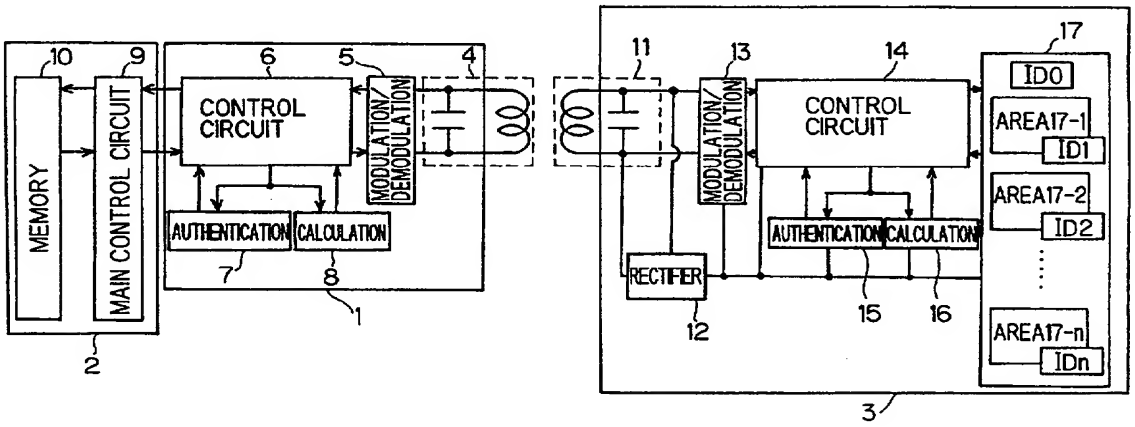
(58) Field of Search
UK CL (Edition R) H4L LADCS LADTA LADTX LADX LASS LAX LECCP LECCX
INT CL[7] G06F 12/08 , G06K 19/07 19/077 , G07F 7/10 , H04L 9/08 9/12 9/14 9/32
ONLINE: WPI, PAJ, EPODOC

(54) Abstract Title

Data transponder with plural memory areas for use with different types of interrogator

(57) A transponder 3 is operable to communicate with a plurality of different types of interrogator managed by a number of providers. The transponder comprises a plurality of storage areas 17-1 to 17-n for storing data used when the transponder communicates individually with the interrogators. A plurality of key signals ID1 -IDN unique to the transponder are stored for each of the storage areas for permitting use of only a particular storage area corresponding to an interrogator with which the transponder is communicating. When communicating with an interrogator, the transponder receives a key signal and compares it with the stored keys to permit access to a storage area. The transponder has a stored ID number ID0 for permitting itself to be identified as well as the additional key signals identifying the memory areas.

FIG.1



GB 2 350 021 A

FIG. 1

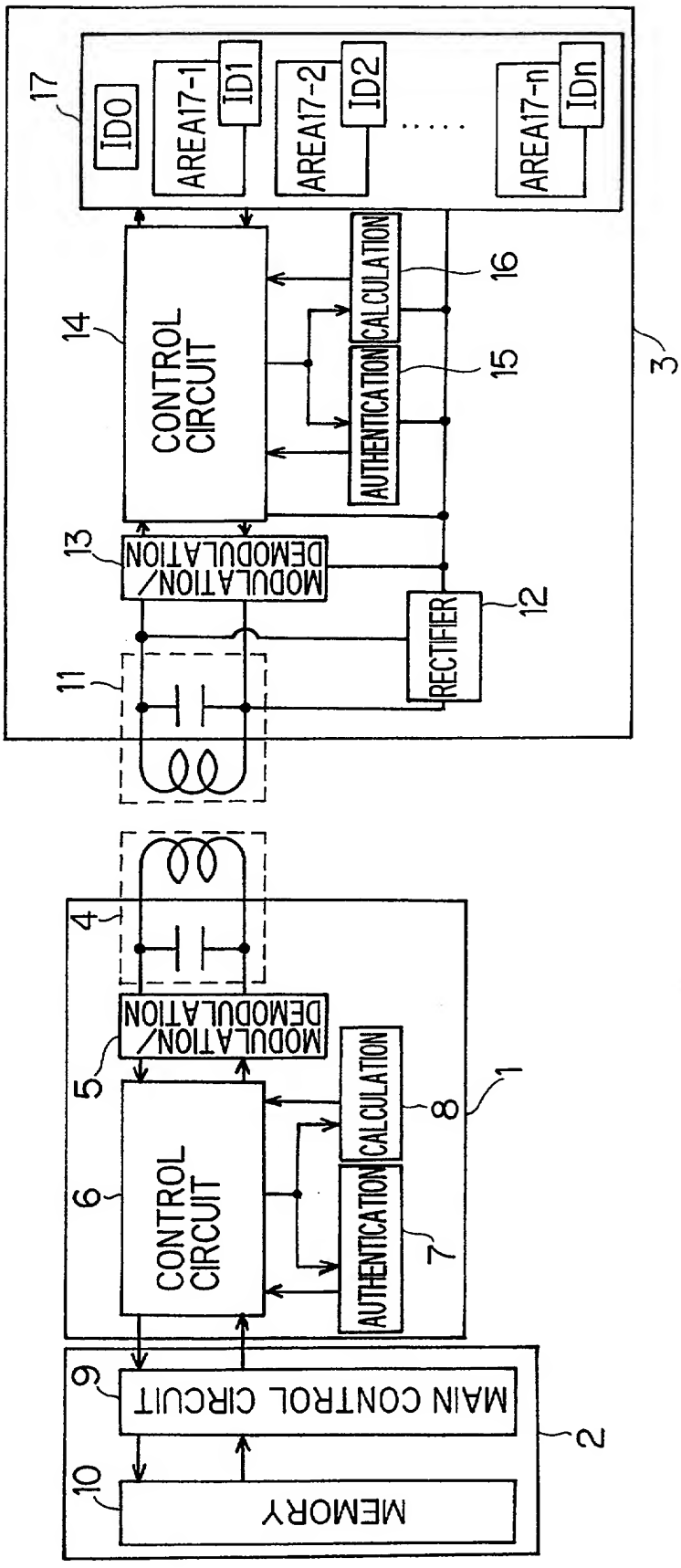

17
ID0
AREA17-1
ID1
AREA17-2
ID2
AREA17-n
IDn
14
CONTROL CIRCUIT
CALCULATION
16
AUTHENTICATION
15
3
13
MODULATION/ DEMODULATION
RECTIFIER
12
11
4
MODULATION/ DEMODULATION
5
6
CONTROL CIRCUIT
CALCULATION
8
1
AUTHENTICATION
7
9
MAIN CONTROL CIRCUIT
2
10
MEMORY

FIG. 2

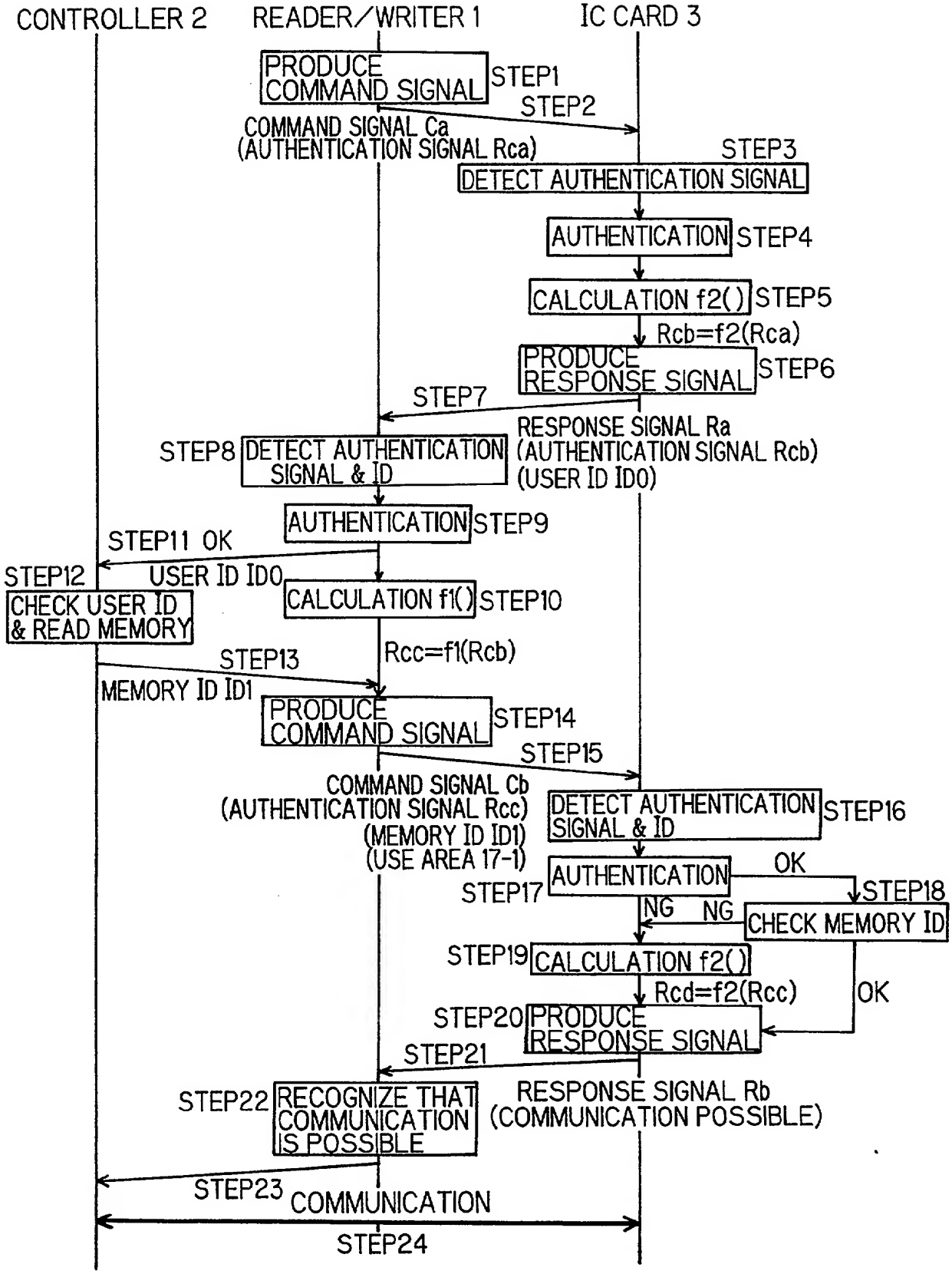

CONTROLLER 2
READER/WRITER 1
IC CARD 3
PRODUCE COMMAND SIGNAL
STEP1
STEP2
COMMAND SIGNAL Ca
(AUTHENTICATION SIGNAL Rca)
STEP3
DETECT AUTHENTICATION SIGNAL
AUTHENTICATION
STEP4
CALCULATION f2()
STEP5
Rcb=f2(Rca)
PRODUCE RESPONSE SIGNAL
STEP6
STEP7
RESPONSE SIGNAL Ra
(AUTHENTICATION SIGNAL Rcb)
(USER ID ID0)
STEP8
DETECT AUTHENTICATION SIGNAL & ID
AUTHENTICATION
STEP9
STEP11 OK
STEP12
USER ID ID0
CHECK USER ID & READ MEMORY
CALCULATION f1()
STEP10
Rcc=f1(Rcb)
STEP13
MEMORY ID ID1
PRODUCE COMMAND SIGNAL
STEP14
STEP15
COMMAND SIGNAL Cb
(AUTHENTICATION SIGNAL Rcc)
(MEMORY ID ID1)
(USE AREA 17-1)
DETECT AUTHENTICATION SIGNAL & ID
STEP16
AUTHENTICATION
OK
STEP17
STEP18
NG
NG
CHECK MEMORY ID
STEP19
CALCULATION f2()
Rcd=f2(Rcc)
OK
STEP20
PRODUCE RESPONSE SIGNAL
STEP21
STEP22
RECOGNIZE THAT COMMUNICATION IS POSSIBLE
RESPONSE SIGNAL Rb
(COMMUNICATION POSSIBLE)
STEP23
COMMUNICATION
STEP24

FIG.3A

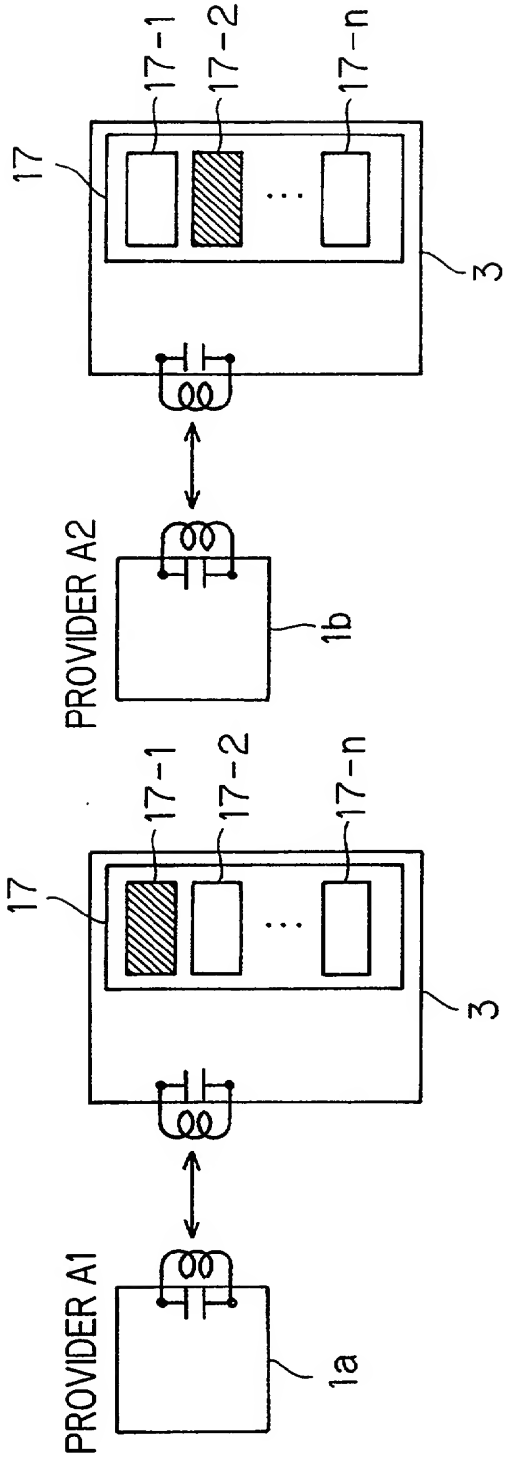


FIG.3B

FIG.4A

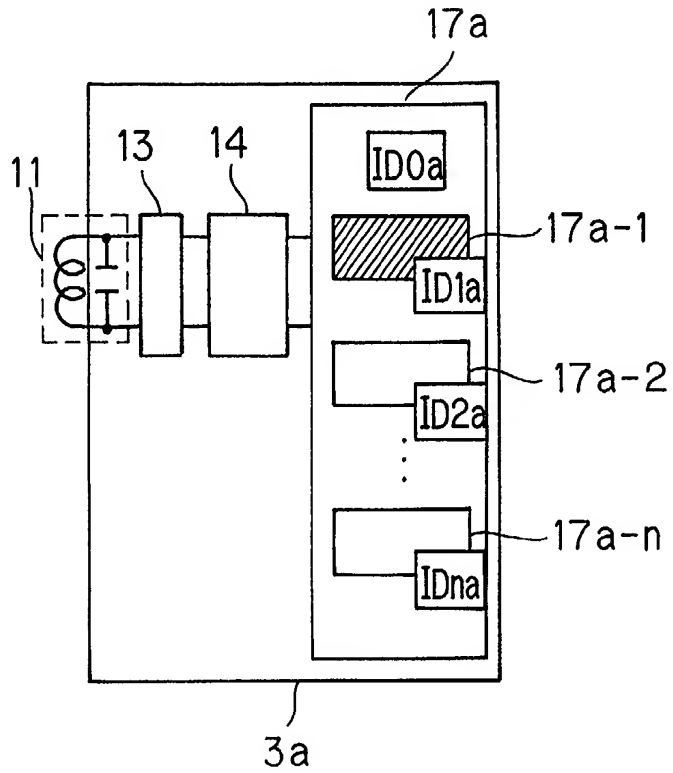

17a
11
13
14
ID0a
17a-1
ID1a
17a-2
ID2a
17a-n
IDna
3a

FIG.4B

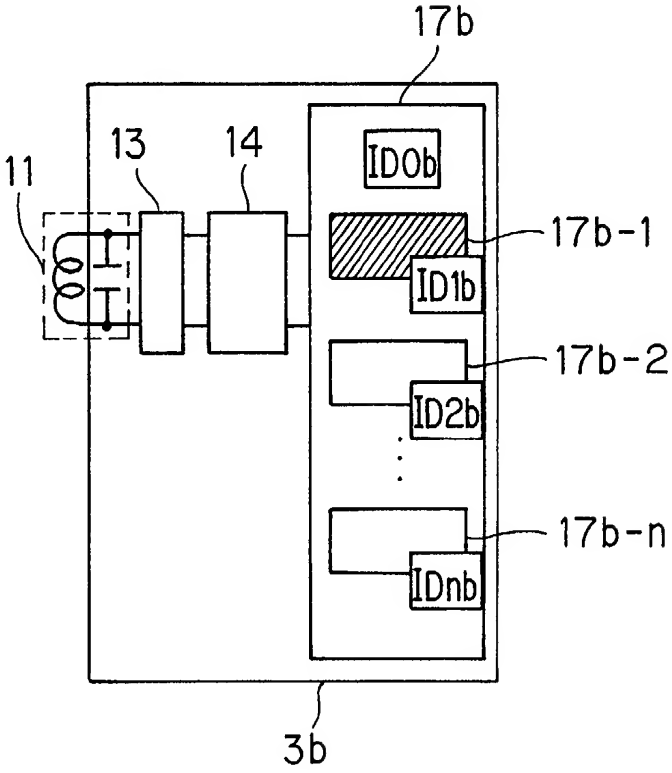

17b
11
13
14
ID0b
17b-1
ID1b
17b-2
ID2b
17b-n
IDnb
3b

FIG.5

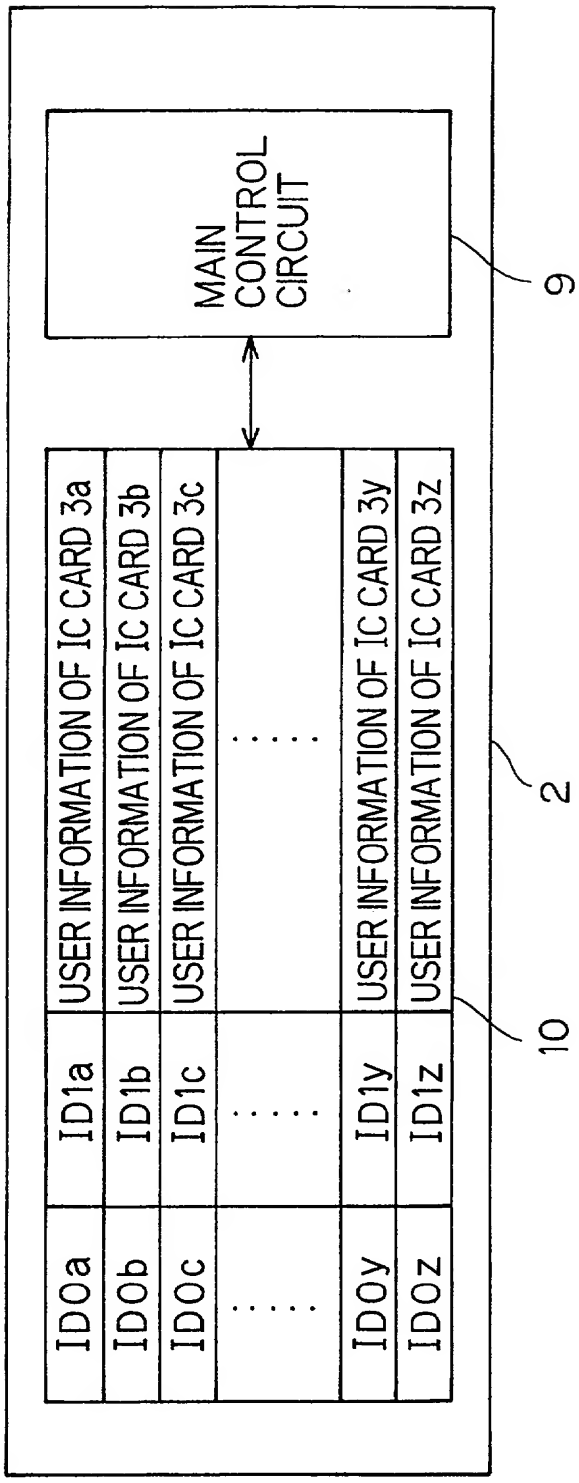

MAIN CONTROL CIRCUIT
9
2
10
ID0a
ID1a
USER INFORMATION OF IC CARD 3a
ID0b
ID1b
USER INFORMATION OF IC CARD 3b
ID0c
ID1c
USER INFORMATION OF IC CARD 3c
ID0y
ID1y
USER INFORMATION OF IC CARD 3y
ID0z
ID1z
USER INFORMATION OF IC CARD 3z

FIG.6

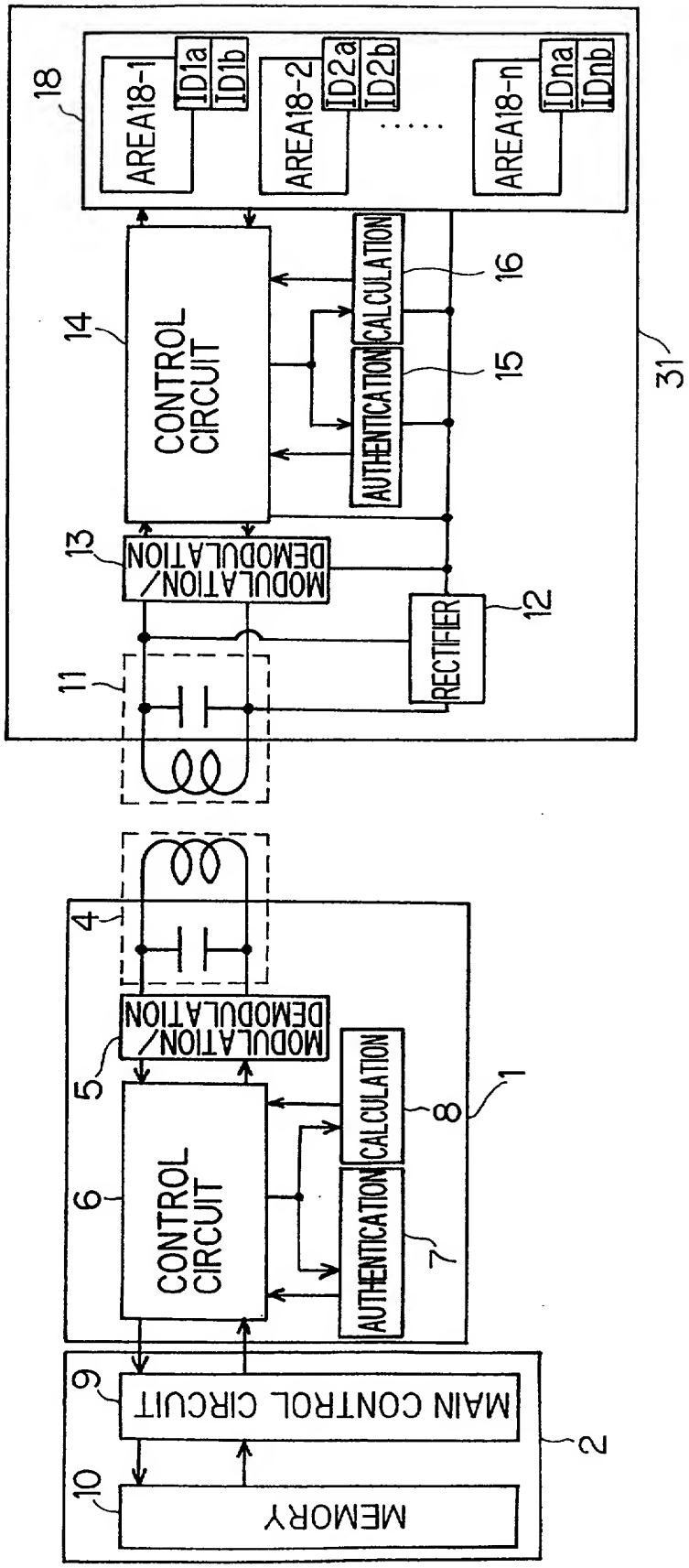

18
AREA18-1
ID1a
ID1b
AREA18-2
ID2a
ID2b
AREA18-n
IDna
IDnb
14
CONTROL CIRCUIT
CALCULATION
16
AUTHENTICATION
15
31
13
MODULATION/ DEMODULATION
RECTIFIER
12
11
4
MODULATION/ DEMODULATION
5
CONTROL CIRCUIT
6
CALCULATION
8
AUTHENTICATION
7
1
9
MAIN CONTROL CIRCUIT
10
MEMORY
2

FIG. 7

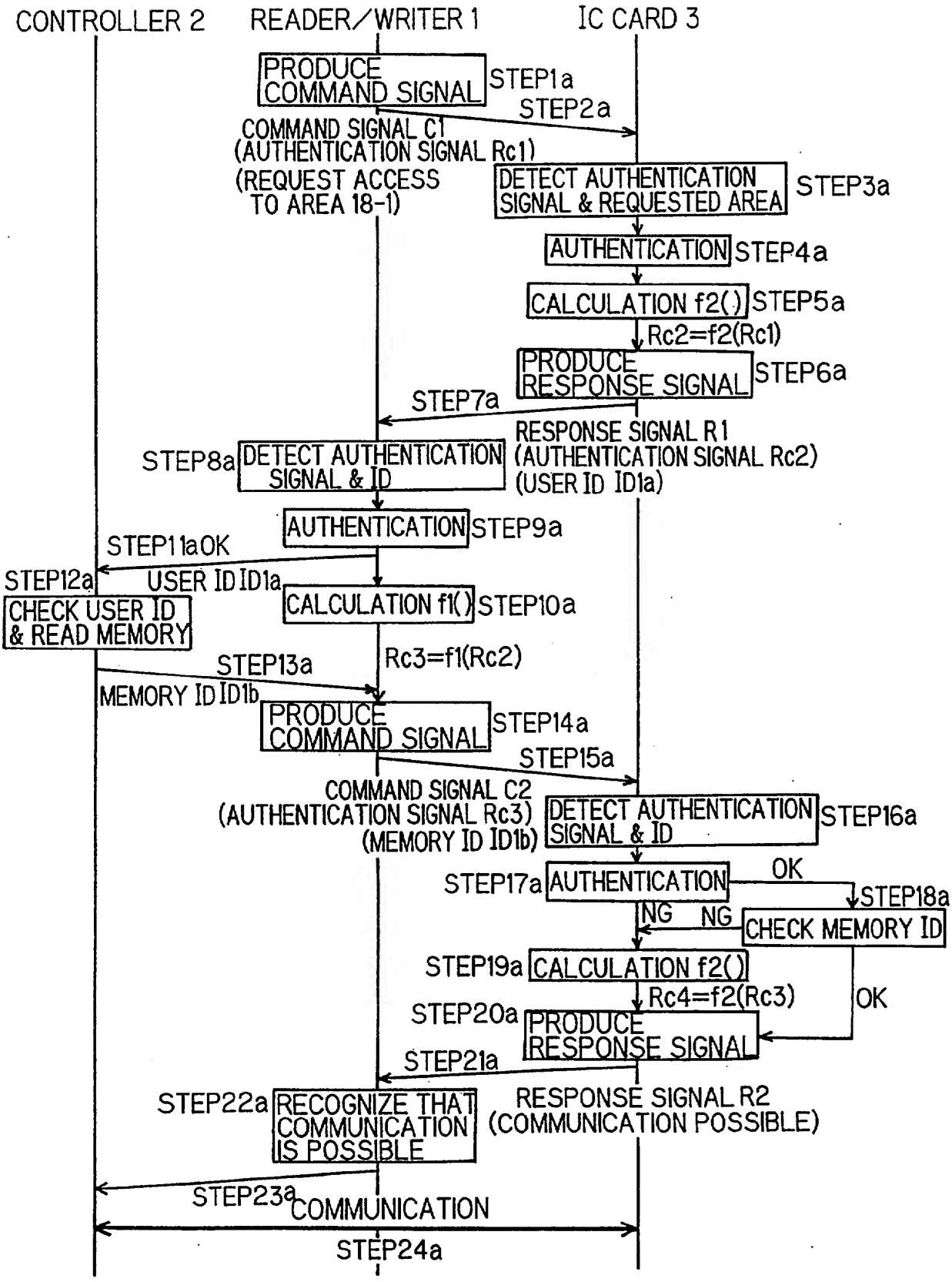

CONTROLLER 2
READER/WRITER 1
IC CARD 3
PRODUCE COMMAND SIGNAL
STEP1a
STEP2a
COMMAND SIGNAL C1
(AUTHENTICATION SIGNAL Rc1)
(REQUEST ACCESS TO AREA 18-1)
DETECT AUTHENTICATION SIGNAL & REQUESTED AREA
STEP3a
AUTHENTICATION
STEP4a
CALCULATION f2()
STEP5a
Rc2=f2(Rc1)
PRODUCE RESPONSE SIGNAL
STEP6a
STEP7a
RESPONSE SIGNAL R1
(AUTHENTICATION SIGNAL Rc2)
(USER ID ID1a)
STEP8a
DETECT AUTHENTICATION SIGNAL & ID
AUTHENTICATION
STEP9a
STEP11a OK
STEP12a
USER ID ID1a
CALCULATION f1()
STEP10a
CHECK USER ID & READ MEMORY
Rc3=f1(Rc2)
STEP13a
MEMORY ID ID1b
PRODUCE COMMAND SIGNAL
STEP14a
STEP15a
COMMAND SIGNAL C2
(AUTHENTICATION SIGNAL Rc3)
(MEMORY ID ID1b)
DETECT AUTHENTICATION SIGNAL & ID
STEP16a
STEP17a
AUTHENTICATION
OK
STEP18a
NG
NG
CHECK MEMORY ID
STEP19a
CALCULATION f2()
Rc4=f2(Rc3)
OK
STEP20a
PRODUCE RESPONSE SIGNAL
STEP21a
STEP22a
RECOGNIZE THAT COMMUNICATION IS POSSIBLE
RESPONSE SIGNAL R2
(COMMUNICATION POSSIBLE)
STEP23a
COMMUNICATION
STEP24a

FIG.8B

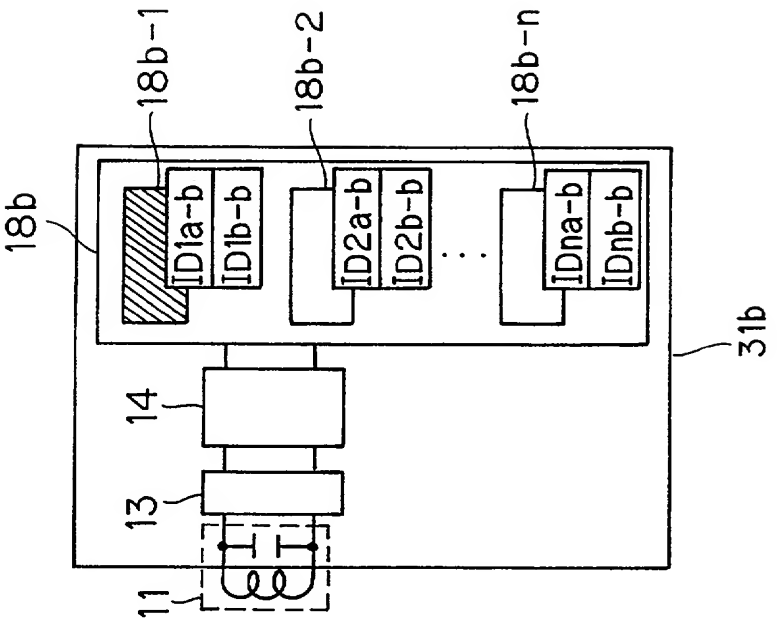

18b-1
18b-2
18b-n
18b
ID1a-b
ID1b-b
ID2a-b
ID2b-b
IDna-b
IDnb-b
31b
14
13
11

FIG.8A

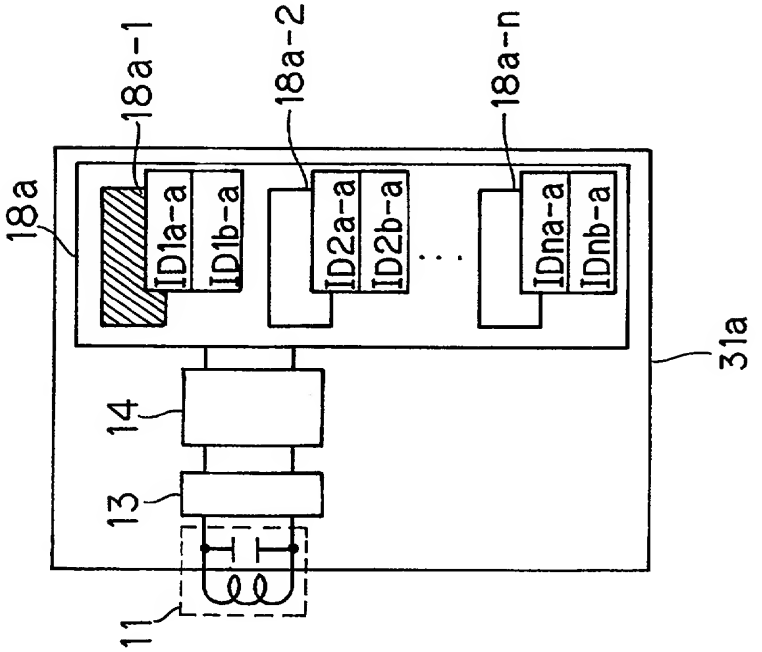

18a-1
18a-2
18a-n
18a
ID1a-a
ID1b-a
ID2a-a
ID2b-a
IDna-a
IDnb-a
31a
14
13
11

FIG. 9

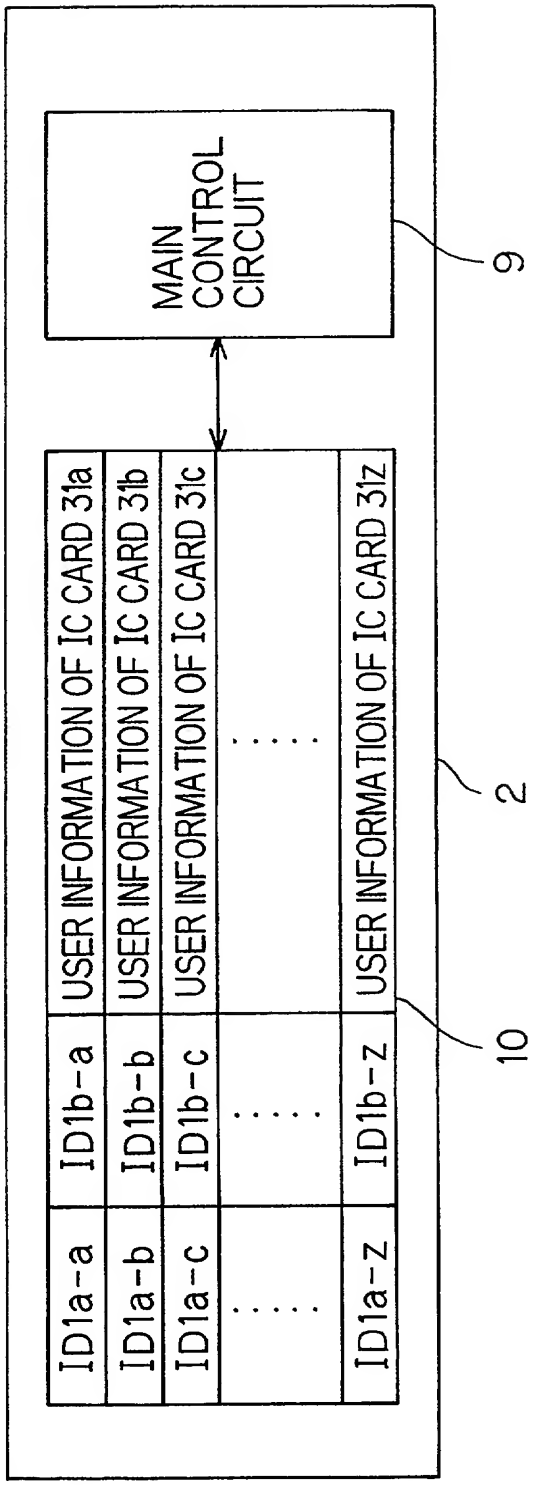

MAIN CONTROL CIRCUIT
9
2
10
ID1a-a
ID1a-b
ID1a-c
ID1a-z
ID1b-a
ID1b-b
ID1b-c
ID1b-z
USER INFORMATION OF IC CARD 31a
USER INFORMATION OF IC CARD 31b
USER INFORMATION OF IC CARD 31c
USER INFORMATION OF IC CARD 31z

FIG.10

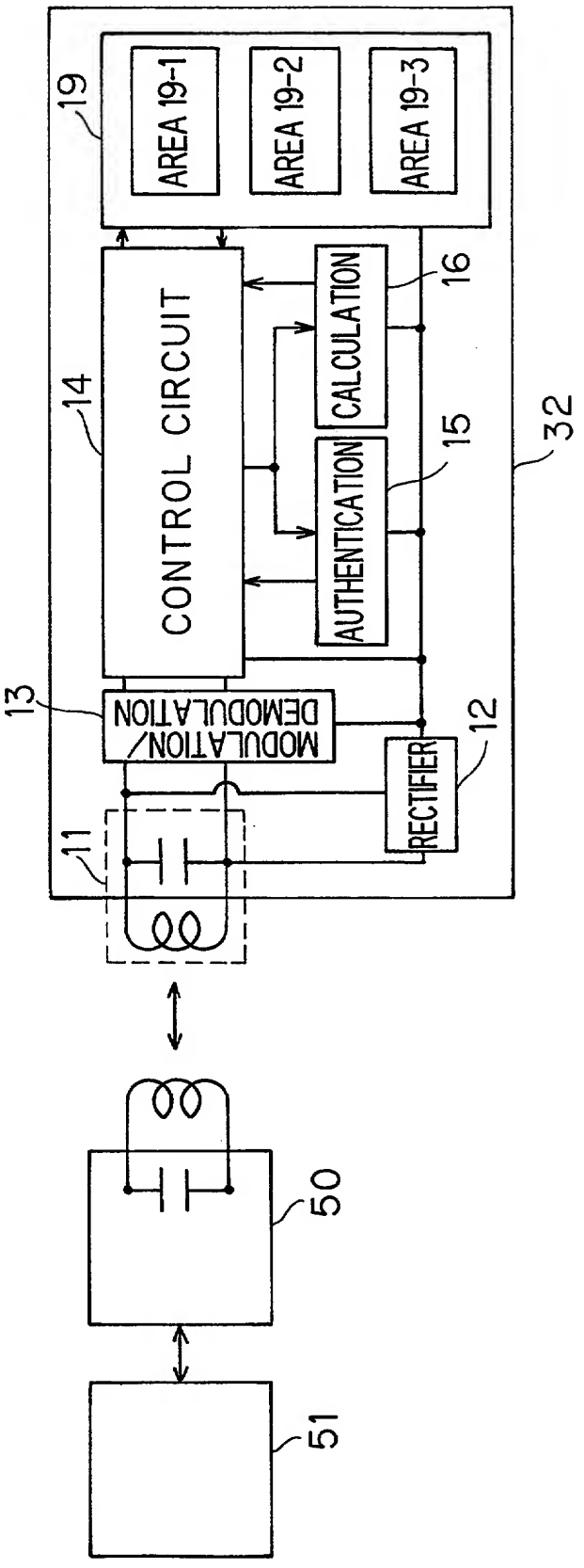
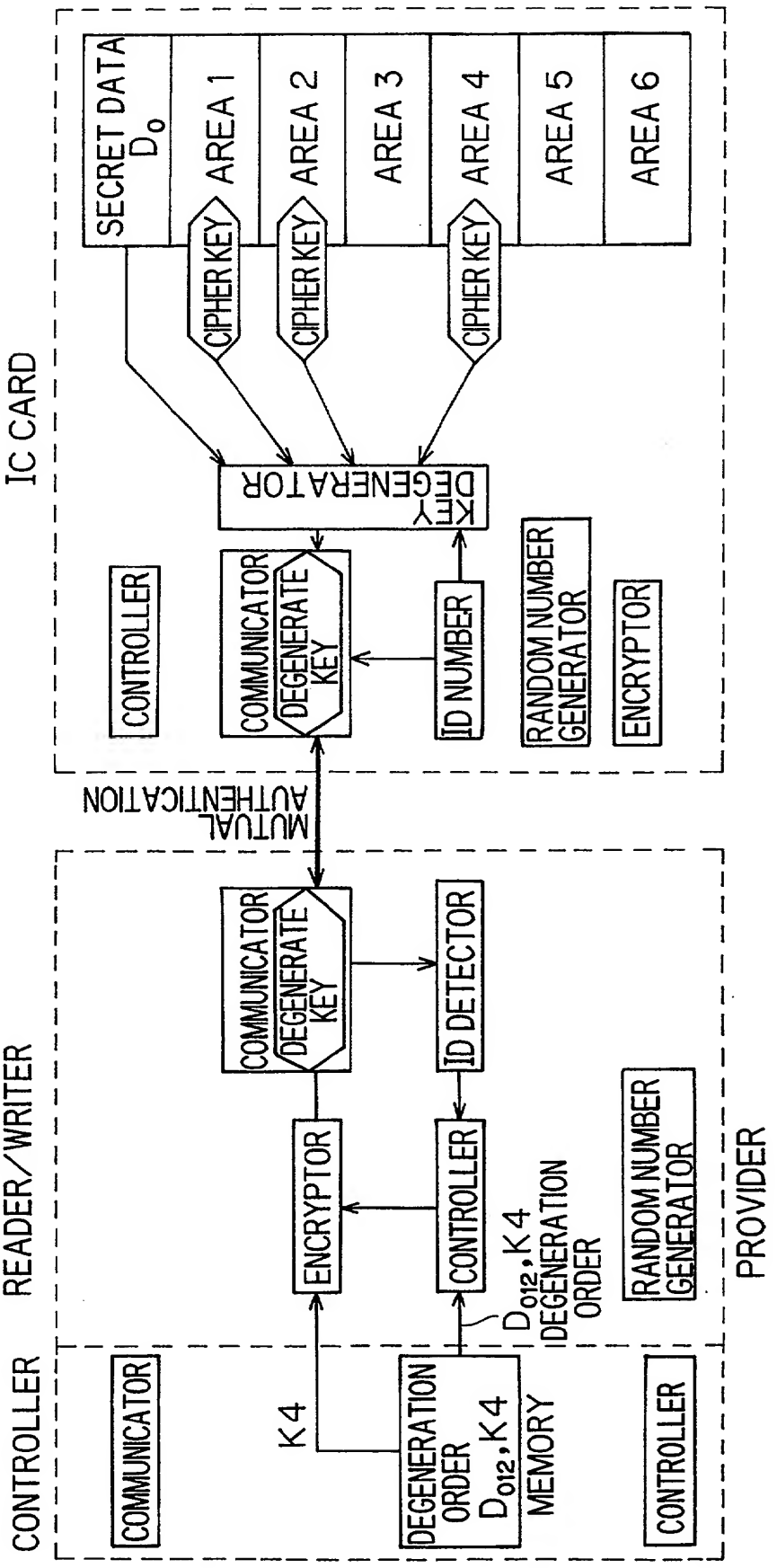

19
AREA 19-1
AREA 19-2
AREA 19-3
CONTROL CIRCUIT
14
CALCULATION
16
AUTHENTICATION
15
32
MODULATION/
DEMODULATION
13
RECTIFIER
12
11
50
51

FIG.11 PRIOR ART



DATA COMMUNICATION TRANSPONDER AND COMMUNICATIONS SYSTEM EMPLOYING IT

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to a data communication transponder, such as a radio-wave tag or IC card, and a communications system employing such a transponder, and in particular to a data communication transponder having a plurality of data storage areas for use in communicating with interrogators of a plurality of providers and a communications system employing such a transponder.

Description of the Prior Art

Nowadays, communications systems are known that permit a single IC card, used as a transponder, to communicate with a plurality of types of reader/writer (interrogator) managed individually by a number of providers. To realize such a communications system, an IC card employed therein has memory divided into a plurality of memory areas allocated individually to a number of providers in order to achieve separate storage of data in communicating with the reader/writers managed individually by those providers. In this system, where a single IC card can communicate with reader/writers managed individually by a number of providers, it is essential, during communication, to permit the use of only a particular memory area allocated to the provider that manages the reader/writer with which a given IC card is currently communicating and simultaneously

prohibit the use of the other memory areas.

To achieve this, each IC card has a plurality of cipher keys stored therein that permit the individual memory areas to be used only when communicating with the reader/writers managed by the corresponding providers to which those memory areas are allocated. An IC card and a reader/writer authenticate each other by the use of such a cipher key. A non-contact communications system involving such a mutual authentication process is proposed in Japanese Laid-Open Patent Application No. H10-327142.

In the communications system proposed in Japanese Laid-Open Patent Application No. H10-327142 mentioned above, as shown in Fig. 11, the cipher keys that are used to permit the use of the individual memory areas secured within an IC card are determined provider by provider. Moreover, once a particular provider is authenticated by the use of the corresponding cipher key, the IC card can recognize, on the basis of the same cipher key, which memory area the provider will request access to. On the other hand, a reader/writer can check whether a given IC card is authentic or not, but cannot identify it (i.e. cannot distinguish one IC card from another). Therefore, to permit reader/writers to identify IC cards, each IC card has also an ID (identification) number unique thereto stored therein.

However, in this system, the cipher keys that are used to permit the use of the memory areas secured within an IC card are determined provider by provider as described above, and thus those cipher keys are not unique to the IC card. Moreover, the ID number stored in an IC card is issued when the IC card is

manufactured, and therefore the ID number, at the same time as it is stored in the IC card, needs to be registered also in individual providers. Thus, every time an IC card is manufactured, its ID number needs to be registered in individual providers. This complicates the management of the communications system.

SUMMARY OF THE INVENTION

An object of the present invention is to provide a data communication transponder and a communications system employing such a transponder that offer higher security by permitting cipher keys, used to permit the use of memory areas secured within an IC card, to be so determined as to be unique to the IC card.

To achieve the above object, according to one aspect of the present invention, a transponder for data communication is provided with: a plurality of storage areas for storing data used when the transponder communicates individually with a plurality of interrogators managed by different parties; a plurality of key signals, unique to the transponder and stored one for each of the storage areas, for permitting the use of only a particular storage area corresponding to the interrogator with which the transponder is currently communicating. Here, the transponder, when communicating with an interrogator, checks the key signal received from the interrogator against the key signals stored in the transponder and, when the received key signal coincides with one of the stored key signals, the transponder is permitted to communicate with the interrogator by using only a particular storage area corresponding to that interrogator.

In this transponder for data communication, the providers that manage the

interrogators that can communicate with the transponder determine the cipher keys, which are used when the transponder communicates with the interrogators, in such a way that those cipher keys are unique to the transponder. When the transponder, having the cipher keys determined in this way, attempts to communicate with one of the interrogators, the interrogator can identify the transponder.

According to another aspect of the present invention, a non-contact communications system is provided with: a plurality of interrogators that are managed by different parties; and a transponder for data communication having a plurality of storage areas for storing data used when the transponder communicates individually with the interrogators and a plurality of key signals, unique to the transponder and stored one for each of the storage areas, for permitting the use of only a particular storage area corresponding to the interrogator with which the transponder is currently communicating. Here, the transponder, when communicating with an interrogator on a non-contact basis, checks the key signal received from the interrogator against the key signals stored in the transponder and, when the received key signal coincides with one of the stored key signals, the transponder is permitted to communicate with the interrogator by using only a particular storage area corresponding to that interrogator.

In this communications system, the providers that manage the interrogators that can communicate with the transponder determine the cipher keys, which are used when the transponder communicates with the interrogators, in such a way that those cipher keys are unique to the transponder. When the transponder,

having the cipher keys determined in this way, attempts to communicate with one of the interrogators, the interrogator can identify the transponder.

BRIEF DESCRIPTION OF THE DRAWINGS

This and other objects and features of the present invention will become clear from the following description, taken in conjunction with the preferred embodiments with reference to the accompanying drawings in which:

Fig. 1 is a block diagram showing the configuration of the communications system of a first embodiment of the invention;

Fig. 2 is a time chart showing the operation of the communications system shown in Fig. 1;

Figs. 3A and 3B are block diagrams showing the relationship between the providers that manage the reader/writers and the memory areas secured within the IC card employed in the communications system shown in Fig. 1;

Figs. 4A and 4B are block diagrams showing the relationship between different IC cards employed in the communications system shown in Fig. 1;

Fig. 5 is a block diagram showing the internal configuration of the controller and the memory employed in the communications system shown in Fig. 1;

Fig. 6 is a block diagram showing the configuration of the communications system of a second embodiment of the invention;

Fig. 7 is a time chart showing the operation of the communications system shown in Fig. 6;

Figs. 8A and 8B are block diagrams showing the relationship between

different IC cards employed in the communications system shown in Fig. 6;

Fig. 9 is a block diagram showing the internal configuration of the controller and the memory employed in the communications system shown in Fig. 6;

Fig. 10 is a block diagram showing the configuration of the communications system of a third embodiment of the invention; and

Fig. 11 is a block diagram showing the configuration of a conventional communications system.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

First, a first embodiment of the present invention will be described with reference to the drawings relevant thereto. Fig. 1 is a block diagram showing the configuration of the communications system of the first embodiment of the invention. Fig. 2 is a time chart showing the operation of the communications system of this embodiment. It is to be noted that, throughout the present specification, the symbol "NG" indicates that an authentication process has found a communication partner to be not authentic, and that the symbol "OK" indicates that an authentication process has found a communication partner to be authentic.

The communications system shown in Fig. 1 has a reader/writer 1 and a controller 2 that together function as an interrogator and an IC card 3 that functions as a transponder. In this communications system, the reader/writer 1 is composed of a tuning circuit 4 that exchanges signals with the IC card 3, a modulation/demodulation circuit 5 that demodulates a response signal received by the tuning circuit 4 and that modulates a command signal produced by a control

circuit 6, a control circuit 6 that produces a command signal, an authentication circuit 7 that receives from the control circuit 6 an authentication signal added to the received response signal and that authenticates the IC card 3 on the basis of the authentication signal, and a calculation circuit 8 that receives from the control circuit 6 the authentication signal added to the received response signal and that performs a predetermined calculation operation f1( ) on the authentication signal. This reader/writer 1 is controlled by the controller 2 that communicates therewith. The controller 2 has a main control circuit 9 that exchanges signals with the control circuit 6 of the reader/writer 1 and that controls the reader/writer 1, and a memory 10 for storing the ID number of and the information related to the owner of the IC card 3.

On the other hand, the IC card 3 is composed of a tuning circuit 11 that exchanges signals with the reader/writer 1, a rectifier circuit 12 that produces a source voltage to be supplied to the individual blocks of the IC card 3 by rectifying the signal tuned in by the tuning circuit 11, a modulation/demodulation circuit 13 that demodulates a command signal received by the tuning circuit 11 and that modulates a response signal produced by a control circuit 14, a control circuit 14 that produces a response signal, an authentication circuit 15 that receives from the control circuit 14 an authentication signal added to the received command signal and that authenticates the reader/writer 1 on the basis of the authentication signal, a calculation circuit 16 that receives from the control circuit 14 the authentication signal added to the received command signal and that performs a predetermined calculation operation f2( ) on the authentication signal, and a memory 17 for

storing the ID number of and the information related to the owner of the IC card 3.

This IC card 3 can communicate with a plurality of reader/writers that are managed individually by different providers. To achieve this, the IC card 3 has its memory 17 divided into memory areas 17-1 to 17-*n* that are allocated for access from the individual providers. Specifically, as shown in Fig. 3A, when the reader/writer 1a managed by a provider A1 is permitted to communicate with the IC card 3, data communication is achieved by reading data from and writing data to one memory area 17-1 secured within the IC card 3, and, as shown in Fig. 3B, when the reader/writer 1b managed by a provider A2 is permitted to communicate with the IC card 3, data communication is achieved by reading data from and writing data to another memory area 17-2 secured within the IC card 3.

Also stored in the memory 17 are ID numbers (hereinafter the "memory IDs") ID1 to ID*n* that are used to permit access to the memory areas 17-1 to 17-*n* and another ID number (hereinafter the "user ID") ID0 that is used to permit each IC card 3 to be identified by the providers. Of these ID numbers ID0 to ID*n*, which are all determined so as to be unique to each IC card 3, the user ID ID0 is determined by the manufacturer when the IC card 3 is manufactured, and the memory IDs ID1 to ID*n* are determined by the individual providers. Specifically, if, as shown in Fig. 4A, the ID numbers that are stored in the memory 17a of one IC card 3a are ID0a and ID1a to ID*n*a, then, as shown in Fig. 4B, the ID numbers that are stored in the memory 17b of another IC card 3b are ID0b and ID1b to ID*n*b, i.e. different values from ID0a and ID1a to ID*n*a.

Moreover, if it is assumed that the provider A, when communicating with

the IC card 3a, uses the memory area 17a-1 and, when communicating with the IC card 3b, uses the memory area 17b-1, then, as shown in Fig. 5, in the memory 10 of the controller 2 managed by the provider A, the user ID ID0a of the IC card 3a, the memory ID ID1a of the memory area 17a-1, and the user information of the IC card 3a are stored as one set of mutually related data, and the user ID ID0b of the IC card 3b, the memory ID ID1b of the memory area 17b-1, and the user information of the IC card 3b are stored as another set of mutually related data.

In this communications system, as shown in Fig. 2, at predetermined intervals, the reader/writer 1 produces a command signal Ca that has an authentication signal (rolling code) Rca added thereto by the control circuit 6 so as to enable the IC card 3 to perform an authentication process (STEP 1). The thus produced command signal Ca is then modulated by the modulation/demodulation circuit 5, and is then transmitted from the tuning circuit 4 to the IC card 3 (STEP 2). Here, the authentication signal Rca that is added to the command signal Ca is an arbitrary signal that has not yet been subjected to the calculation operation f1( ) by the calculation circuit 8.

When the IC card 3 receives this command signal Ca through its tuning circuit 11, the rectifier circuit 12 produces a source voltage therefrom, and the modulation/demodulation circuit 13 demodulates and feeds it to the control circuit 14. The control circuit 14, on detecting the authentication signal Rca added to the command signal Ca, feeds the authentication signal Rca to the authentication circuit 15 to check whether or not this authentication signal Rca has already been subjected to the calculation operation f1( ) within the reader/writer 1 (STEP 3).

Here, since this authentication signal Rca has not yet been subjected to the calculation operation f1( ), the authentication process results in "NG", and thus the IC card 3 does not authenticate the reader/writer 1 (STEP 4).

At the same time, the authentication signal Rca detected by the control circuit 14 is fed to the calculation circuit 16 so as to be subjected to the calculation operation f2( ) (STEP 5). The signal f2(Rca) resulting from the calculation operation f2( ) performed by the calculation circuit 16 is, as an authentication signal Rcb, fed to the control circuit 14 so as to be added to a response signal Ra that will be transmitted to the reader/writer 1. Moreover, the control circuit 14 adds to this response signal Ra the data of the user ID ID0 stored in the memory 17 (STEP 6). The response signal Ra thus produced is modulated by the modulation/demodulation circuit 13, and is then transmitted from the tuning circuit 11 to the reader/writer 1 (STEP 7).

When the reader/writer 1 receives this response signal Ra through its tuning circuit 4, the modulation/demodulation circuit 5 demodulates and feeds it to the control circuit 6. The control circuit 6 detects the authentication signal Rcb and the user ID ID0 added to the response signal Ra (STEP 8), and then feeds the authentication signal Rcb to the authentication circuit 7 to check whether or not this authentication signal Rcb has already been subjected to the calculation operation f2( ) within the IC card 3. Here, since the authentication signal Rcb = f2(Rca) has already been subjected to the calculation operation f2( ), the reader/writer 1 authenticates the IC card 3 (STEP 9).

Here, the authentication signal Rcb detected by the control circuit 6 is fed to

the calculation circuit 8 so as to be subjected to the calculation operation f1( ). The signal obtained by subjecting the authentication signal Rcb to the calculation operation f1( ) is, as an authentication signal Rcc, fed to the control circuit 6 (STEP 10). However, if the authentication process in STEP 9 results in "NG", the reader/writer 1 does not communicate with the controller 2; if this authentication process results in "OK", the user ID ID0 detected by the control circuit 6 is fed to the main control circuit 9 of the controller 2 (STEP 11), and the memory ID ID1 that is stored in the memory 10 so as to correspond to that user ID ID0 and that will be used to permit the use of the memory area 17-1 of the IC card 3 is read (STEP 12). Then, the controller 2 feeds the memory ID ID1 read from the memory 10 from its main control circuit 9 to the control circuit 6 of the reader/writer 1 (STEP 13).

Here, if the authentication process performed by the authentication circuit 7 results in "OK", the control circuit 6 feeds the modulation/demodulation circuit 5 with a command signal Cb to which the memory ID ID1, the authentication signal Rcc, and a signal requesting the use of the memory area 17-1 are added; if the authentication process performed by the authentication circuit 7 results in "NG", or if no user ID ID0 is stored in the memory 10, the control circuit 6 feeds the modulation/demodulation circuit 5 with a command signal Cb1 to which the authentication signal Rcc is added (STEP 14). The command signal Cb or Cb1 thus produced by the control circuit 6 is then fed to the modulation/demodulation circuit 5, and is then transmitted from the tuning circuit 4 (STEP 15).

When the IC card 3 receives the command signal Cb through its tuning

circuit 11, the rectifier circuit 12 produces a source voltage therefrom, and the modulation/demodulation circuit 13 demodulates and feeds it to the control circuit 14. The control circuit 14 detects the authentication signal Rcc and the memory ID ID1 added to the command signal Cb, and recognizes that the reader/writer 1 will use the memory area 17-1 (STEP 16). Then, the authentication signal Rcc is fed to the authentication circuit 15 to check whether or not this authentication signal Rcc has already been subjected to the calculation operation f1( ) within the reader/writer 1. It is to be noted that, although not shown in the time chart of Fig. 2, when the IC card 3 receives the command signal Cb1, the reader/writer 1, the controller 2, and the IC card 3 repeat the operations starting with STEP 3. Here, since it is assumed that the IC card 3 has received the command signal Cb, the authentication circuit 15 checks whether the reader/writer 1 is authentic or not on the basis of the authentication signal Rcc (STEP 17).

Here, if the authentication process results in "OK", the control circuit 14 compares the memory ID received from the reader/writer 1 with the memory ID stored in the memory area 17-1 within the memory 17 to check whether they coincide or not (STEP 18). The operation flow then proceeds, if the two memory IDs coincide, to STEP 20 and, otherwise, to STEP 19. On the other hand, if the authentication process in STEP 17 results in "NG", or if the two memory IDs do not coincide in STEP 18, the authentication signal Rcc detected by the control circuit 14 is fed to the calculation circuit 16 so as to subject it to the calculation operation f2( ). The signal f2(Rcc) obtained by subjecting the authentication signal Rcc to the calculation operation f2( ) is, as an authentication signal Rcd, fed to the control

circuit 14 (STEP 19), and then the operation flow proceeds to STEP 20.

When the operation flow, on completion of the operation in STEP 18 or 19, proceeds to STEP 20, the control circuit 14 produces, if the authentication process results in "OK", a response signal Rb for notifying the reader/writer 1 that communication is possible or, if the authentication process results in "NG", a response signal Rb1 to which the authentication signal Rcd and the user ID ID0 are added, and feeds the produced signal to the modulation/demodulation circuit 13. Here, since the authentication signal Rcc = f1(Rcb), and the memory ID received from the reader/writer 1 is ID1 and thus coincides with the memory ID of the memory area 17-1, the response signal Rb for notifying the reader/writer 1 that communication is possible is produced in STEP 20. When the response signal Rb or Rb1 is fed to the modulation/demodulation circuit 13, it is modulated thereby and is then transmitted from the tuning circuit 11 (STEP 21).

When the reader/writer 1 receives the response signal Rb through its tuning circuit 4, the modulation/demodulation circuit 5 demodulates and feeds it to the control circuit 6. In response to the response signal Rb, the control circuit 6 permits access to the memory area 17-1 within the IC card 3, and recognizes that communication is now possible (STEP 22). It is to be noted that, although not shown in the time chart of Fig. 2, when the reader/writer 1 receives the response signal Rb1, the reader/writer 1, the controller 2, and the IC card 3 repeat the operations starting with STEP 8.

Here, it is assumed that the reader/writer 1 has received the response signal Rb, and therefore the control circuit 6 then makes the main control circuit 9 of the

controller 2 recognize that communication is now possible with the IC card 3 (STEP 23). On recognizing that communication is possible with the IC card 3, the controller 2 communicates with the IC card 3 through the reader/writer 1, and, meanwhile, data is read from or written to the memory area 17-1 of the IC card 3 (STEP 24).

Next, a second embodiment of the present invention will be described with reference to the drawings relevant thereto. Fig. 6 is a block diagram showing the configuration of the communications system of this embodiment. Fig. 7 is a time chart showing the operation of the communications system of this embodiment. In the communications system of this embodiment, the reader/writer and the controller shown in Fig. 6 have the same internal configuration as the reader/writer 1 and the controller 2 in the communications system shown in Fig. 1. Moreover, in the block constituting the IC card in Fig. 6, such elements as are found also in the IC card 3 in the communications system shown in Fig. 1 are identified with the same reference numerals and symbols, and their detailed descriptions will not be repeated.

The IC card 31 shown in Fig. 6 has a memory 18 divided into memory areas 18-1 to 18-*n*, a tuning circuit 11, a rectifier circuit 12, a modulation/demodulation circuit 13, a control circuit 14, an authentication circuit 15, and a calculation circuit 16. This IC card 31, like the IC card 3 in the first embodiment, can communicate with a plurality of reader/writers managed by different providers, and thus has its memory 18 divided into memory areas 18-1 to 18-*n* that are allocated for access from the individual providers.

In the memory areas 18-1 to 18-*n* are stored ID numbers (hereinafter the "user IDs") ID1a to ID*n*a that are used to permit each ID card 3 to be identified by the individual providers and ID numbers (hereinafter the "memory IDs") ID1b to ID*n*b that are used to permit access to the memory areas 18-1 to 18-*n*. Thus, the user IDs ID1a to ID*n*a and the memory IDs ID1b to ID*n*b are stored in the memory 18. The user IDs ID1a to ID*n*a and the memory IDs ID1b to ID*n*b are determined so as to be unique to each IC card 31 by the individual providers after the manufacture of the IC card 31.

Moreover, if it is assumed that, as shown in Figs. 8A and 8B, a provider B, when communicating with an IC card 31a, uses the memory area 18a-1 within the memory 18a and, when communicating with an IC card 31b, uses the memory area 18b-1 within the memory 18b, then, as shown in Fig. 9, in the memory 10 of the controller 2, the user ID ID1a-a and the memory ID ID1b-a of the IC card 31a are stored as one set of mutually related data, and the user ID ID1a-b and the memory ID ID1b-b of the IC card 31b are stored as another set of mutually related data.

The operation of this communications system will be described below with reference to Fig. 7. It is to be noted that, in the following descriptions, such operations as are found also in Fig. 2 are indicated as such, and their detailed descriptions will not be repeated. First, in STEPs 1a and 2a, the reader/writer 1 performs the same operations as in STEPs 1 and 2 shown in Fig. 2 to transmit a command signal C1 having an authentication signal Rc1 added thereto to the IC card 31. Here, the command signal C1 has also a signal requesting access to the memory area 18-1 added thereto.

When the IC card 31 receives this command signal C1 through its tuning circuit 11, then, in STEP 3a, the control circuit 14 recognizes that the reader/writer 1 is requesting access to the memory area 18-1 and also, as in STEP 3 in Fig. 2, detects the authentication signal Rc1 and feeds it to the authentication circuit 15. Then, in STEPs 4a and 5a, the same operations as in STEPs 4 and 5 in Fig. 2 are performed.

Then, the control circuit 14 adds to a response signal R1 the authentication signal Rc2 = f2(Rc1) produced by the calculation circuit 16 on the basis of the authentication signal Rc1, and adds thereto also the user ID ID1a of the memory area 18-1 read from the memory 18 (STEP 6a). The response signal R1 thus produced is modulated by the modulation/demodulation circuit 13 and is then transmitted from the tuning circuit 11 to the reader/writer 1 (STEP 7a).

When the reader/writer 1 receives this response signal R1 through its tuning circuit 4, then, in STEPs 8a to 14a, the same operations as in STEPs 8 to 14 in Fig. 2 are performed. Specifically, the control circuit 6 detects the user ID ID1a and the authentication signal Rc2 added to the response signal R1, and then the authentication circuit 7 performs an authentication process on the basis of the authentication signal Rc2. Here, if the authentication process results in "NG", the reader/writer 1 does not communicate with the controller 2; instead, the operation flow proceeds to STEP 10a, so that an authentication signal Rc3 = f1(Rc2) is produced by the calculation circuit 8, and then a command signal C2a is produced to which the authentication signal Rc3 is added. On the other hand, if the authentication process results in "OK", the operation flow proceeds to STEP 11a, so

that the controller 2 reads, within the memory 10, the memory ID ID1b that corresponds to the user ID ID1a and feeds it to the reader/writer 1, and then a command signal C2 is produced to which the authentication signal Rc3 produced by the calculation circuit 8 and the memory ID ID1b are added. When there is no user ID ID1a in the memory 10, the control circuit 6 produces the command signal C2a mentioned above.

When the command signal C2 or C2a is produced in this way, this command signal is transmitted to the IC card 31 (STEP 15a). Here, since the authentication signal Rc2 = f2(Rc1) has already been subjected to the calculation operation f2( ), the reader/writer 1 authenticates the IC card 31. Thus, the command signal C2 is transmitted to the IC card 31.

The operations performed in STEP 16a and the following steps are almost the same as those performed in STEP 16 and the following steps in Fig. 2 except that different symbols are used. Therefore, the descriptions of those steps will be given below in simplified form.

When the IC card 31 receives the command signal C2, the control circuit 14 detects the authentication signal Rc3 and the memory ID ID1b added to the command signal C2 (STEP 16a). It is to be noted that, if the IC card 31 receives the command signal C2a here, just as in the first embodiment, the reader/writer 1, the controller 2, and the IC card 31 repeat the operations starting with STEP 3a. Then, the authentication circuit 15 checks whether or not the authentication signal Rc3 has already been subjected to the calculation operation f1( ) within the reader/writer 1 to check whether the reader/writer 1 is authentic or not (STEP 17a).

Here, if the authentication process results in "OK", the control circuit 14 compares the memory ID received from the reader/writer 1 with the memory ID stored in the memory area 18-1 to check whether they coincide or not (STEP 18a), and then the operation flow proceeds, if the two memory IDs coincide, to STEP 20a and, otherwise, to STEP 19a. On the other hand, if the authentication process in STEP 17a results in "NG", or if the two memory IDs do not coincide in STEP 18a, the authentication signal Rc3 detected by the control circuit 14 is fed to the calculation circuit 16. In this case, the calculation circuit 16 produces an authentication signal Rc4 = f2(Rc3) (STEP 19a), and then the operation flow proceeds to STEP 20a.

When the operation flow, on completion of the operation in STEP 18a or 19a, proceeds to STEP 20a, the control circuit 14 produces, if the authentication process results in "OK", a response signal R2 for notifying the reader/writer 1 that communication is possible or, if the authentication process results in "NG", a response signal R2a to which the authentication signal Rc4 and the user ID ID1a are added, and feeds the produced signal to the reader/writer 1. Here, since the authentication signal Rc3 = f1(Rc2), and the memory ID received from the reader/writer 1 is ID1b and thus coincides with the memory ID of the memory area 18-1, the response signal R2 for notifying the reader/writer 1 that communication is possible is transmitted in STEP 21a.

When the reader/writer 1 receives the response signal R2, the control circuit 6, on the basis of the response signal R2, permits access to the memory area 18-1 within the IC card 31, and recognizes that communication is now possible (STEP

22a). It is to be noted that, just as in the first embodiment, when the reader/writer 1 receives the response signal R2a, the reader/writer 1, the controller 2, and the IC card 31 repeat the operations starting with STEP 8a.

Here, it is assumed that the reader/writer 1 has received the response signal R2, and therefore the control circuit 6 then makes the main control circuit 9 of the controller 2 recognize that communication is now possible with the IC card 31 (STEP 23a). On recognizing that communication is possible with the IC card 31, the controller 2 communicates with the IC card 31 through the reader/writer 1, and, meanwhile, data is read from or written to the memory area 18-1 of the IC card 31 (STEP 24a).

In both of the first and second embodiments, if authentication processes are performed a plurality of times between the reader/writer and the IC card and no authentication results, then an error message is transmitted to the controller and communication is terminated. Similarly, if verification of an ID number is performed a plurality of times in the IC card or in the controller and the ID is found to be coincident with none stored, then an error message is transmitted to the controller and communication is terminated.

Next, a third embodiment of the present invention will be described with reference to the drawings relevant thereto. Fig. 10 is a block diagram showing the configuration of the communications system of this embodiment. In the communications system of this embodiment, the reader/writer and the controller shown in Fig. 10 have the same internal configuration as the reader/writer 1 and the controller 2 in the communications system shown in Fig. 1. Moreover, in the

block constituting the IC card in Fig. 10, such elements as are found also in the IC card 3 in the communications system shown in Fig. 1 are identified with the same reference numerals and symbols, and their detailed descriptions will not be repeated.

The IC card 32 shown in Fig. 10 has a memory 19 divided into memory areas 19-1 to 19-3, a tuning circuit 11, a rectifier circuit 12, a modulation/demodulation circuit 13, a control circuit 14, an authentication circuit 15, and a calculation circuit 16. This IC card 32, like the IC card 3 in the first embodiment, can communicate with a plurality of reader/writers managed individually by different providers C1, C2, and C3, and thus has its memory 19 divided into memory areas 19-1 to 19-3 that are allocated for access from the individual providers C1, C2, and C3.

For example, the provider C1 handles the IC card 32 as a prepaid card for storing a count of points representing an amount of money, and the IC card 32 incorporates, within its memory 19, a down counter (not shown) in which the count of points is stored in the form of a number of bits so as to be decreased according as the points are used. This down counter is initialized by a reset signal fed from the control circuit 14. Now, suppose that the IC card 32 is brought close to the reader/writer 50 managed by the provider C1, and, as the result of the authentication processes as performed in the first or second embodiments, the reader/writer 50 and the IC card 32 authenticate each other and access to the memory area 19-1 is permitted, making it possible for the controller 51 and the IC card 32 to communicate with each other through the reader/writer 50.

Now, a description will be given of how this system works when the user D of the IC card 32 uses the IC card 32 to pay bills, for example, at a gas station. First, the data of the number of remaining points for the user D stored in the memory (not shown) provided within the controller 51 is added to a command signal requesting the reading of the number of bits stored in the down counter, and this command signal is transmitted from the controller 51 through the reader/writer 50 to the IC card 32. Here, the controller 51 calculates the number of remaining points for the user D after the payment, and stores the result in the main control circuit (not shown).

When the IC card 32 receives this command signal, the control circuit 14 feeds the memory area 19-1 with a signal requesting the down counter to be enabled to be read. When the memory area 19-1 receives this signal, the down counter is enabled to be read, and the control circuit 14 counts the number of bits stored therein. Moreover, the control circuit 14 compares the number of remaining points for the user D stored in the memory within the controller 51 and added to the command signal with the number of points detected from a response signal to check whether they coincide or not. If the two numbers coincide, the control circuit 14 transmits through the reader/writer 50 to the controller 51 a response signal indicating the coincidence of the two numbers.

When the controller 51 receives this response signal, it transmits through the reader/writer 50 to the IC card 32 a command signal requesting the number of bits stored in the down counter to be decreased by the number of bits corresponding to the bill to be paid. Here, the controller 51 calculates the number

of remaining points for the user D after the payment, and stores the result in the main control circuit (not shown). When the IC card 32 receives this command signal, the control circuit 14 feeds the memory area 19-1 with a signal requesting the down counter to be enabled to be written. When the memory area 19-1 receives this signal, the down counter is enabled to be written, and the number of bits stored in the down counter is decreased by the number of bits detected from the command signal.

When some of the remaining points are deleted in this way, the control circuit 14 calculates the number of bits stored in the down counter after the deletion, and a response signal to which the data of the number of points corresponding to that number of bits is added is transmitted through the reader/writer 50 to the controller 51. The controller 51 compares the number of points stored in the main control circuit with the number of points detected from the response signal, and, when they coincide, it transmits a command signal indicating the coincidence of the two numbers to the IC card 32, and stores this number in the memory of the controller 51. Then, the controller 51 terminates communication.

Next, a description will be given of how this system works when, after the IC card 32 and the reader/writer 50 have authenticated each other to make it possible for them to communicate with each other, the user D deposits money to increase the number of remaining points. First, the data of the number of remaining points for the user D stored in the memory provided within the controller 51 is added to a command signal requesting the reading of the number of

bits stored in the down counter, and this command signal is transmitted from the controller 51 through the reader/writer 50 to the IC card 32.

When the IC card 32 receives this command signal, the control circuit 14 feeds the memory area 19-1 with a signal requesting the down counter to be enabled to be read. When the memory area 19-1 receives this signal, the down counter is enabled to be read, and the control circuit 14 counts the number of bits stored therein. Moreover, the control circuit 14 compares the number of remaining points for the user D stored in the memory within the controller 51 and added to the command signal with the number of points detected from a response signal to check whether they coincide or not. If the two numbers coincide, the control circuit 14 transmits through the reader/writer 50 to the controller 51 a response signal indicating the coincidence of the two numbers.

When the controller 51 receives this response signal, it transmits through the reader/writer 50 to the IC card 32 a command signal requesting the number of bits stored in the down counter to be changed to a number corresponding to the number of points after the depositing of money. Here, the controller 51 calculates the number of remaining points for the user D after the depositing, and stores the result in the main control circuit. When the IC card 32 receives this command signal, the control circuit 14 feeds the memory area 19-1 with a signal requesting the down counter to be enabled to be written. When the memory area 19-1 receives this signal, the down counter is enabled to be written. Thereafter, the control circuit 14 first feeds the down counter with a reset signal to initialize it, and then decreases the number of bits stored in the down counter until it becomes

equal to the number of bits detected from the command signal.

When the number of remaining points is changed in this way, the control circuit 14 calculates the number of bits stored in the down counter after the change, and a response signal to which the data of the number of points corresponding to that number of bits is added is transmitted through the reader/writer 50 to the controller 51. The controller 51 compares the number of points stored in the main control circuit with the number of points detected from the response signal, and, when they coincide, it transmits a command signal indicating the coincidence of the two numbers to the IC card 32, and stores this number in the memory of the controller 51. Then, the controller 51 terminates communication.

The embodiments described above all deal with transponders for data communication, such as IC cards, that achieve communication on a non-contact basis. However, the present invention is applicable also to transponders for data communication that achieve communication on a wired (i.e. direct-contact) basis. In that case, instead of using tuning circuits as are used in the first to third embodiments to exchange signals, input/output interfaces are provided in the transponder and the interrogator to allow them to communicate with each other.

According to the present invention, in a transponder for data communication, key signals that are used to permit the use of storage areas are determined so as to be unique to the transponder so that the use of the storage areas will be permitted on the basis of those key signals. By the use of this transponder for data communication, it is possible to build a communications system that offers higher security. Moreover, this transponder for data

communication is provided with an authentication circuit for producing a signal requesting an interrogator to permit communication therewith, and therefore no communication is possible unless the interrogator authenticates the transponder. Thus, it is possible to realize a communications system that offers higher security.

What is claimed is:

1. A transponder for data communication, comprising:

a plurality of storage areas for storing data used when the transponder communicates individually with a plurality of interrogators managed by different parties;

a plurality of key signals, unique to the transponder and stored one for each of the storage areas, for permitting use of only a particular storage area corresponding to an interrogator with which the transponder is currently communicating,

wherein the transponder, when communicating with an interrogator, checks a key signal received from the interrogator against the key signals stored in the transponder and, when the received key signal coincides with one of the stored key signals, the transponder is permitted to communicate with the interrogator by using only a particular storage area corresponding to that interrogator.

2. A transponder for data communication as claimed in claim 1, further comprising:

an authentication circuit for generating a signal that is transmitted to the interrogator in order to request the interrogator to permit communication.

3. A transponder for data communication as claimed in claim 1, further comprising:

an authentication circuit for detecting a signal that is transmitted from the

interrogator in order to request the transponder to permit communication, for checking whether the interrogator is authentic or not on a basis of the detected signal, and for permitting communication if the interrogator is found to be authentic.

4. A transponder for data communication as claimed in claim 1, further comprising:

a calculation circuit for performing a predetermined calculation operation on a signal added to a command signal transmitted from the interrogator in order to request the transponder to permit communication and for adding a resulting signal to a response signal that is transmitted back to the interrogator; and

an authentication circuit for checking whether the interrogator is authentic or not on a basis of the signal added to the command signal transmitted from the interrogator in order to request the transponder to permit communication,

wherein the signal obtained through the predetermined calculation operation performed by the calculation circuit so as to be added to the response signal is used as a signal on a basis of which the interrogator checks whether the transponder is authentic or not.

5. A transponder for data communication as claimed in claim 1,

wherein at least one of the storage areas is composed of a count storage member in which a count is stored that is updated in response to a count updating command transmitted from the interrogator when the transponder communicates

with the interrogator by using that storage area.

6. A transponder for data communication as claimed in claim 5, further comprising:

an authentication circuit for generating a signal that is transmitted to the interrogator in order to request the interrogator to permit communication.

7. A transponder for data communication as claimed in claim 5, further comprising:

an authentication circuit for detecting a signal that is transmitted from the interrogator in order to request the transponder to permit communication, for checking whether the interrogator is authentic or not on a basis of the detected signal, and for permitting communication if the interrogator is found to be authentic.

8. A transponder for data communication as claimed in claim 5, further comprising:

a calculation circuit for performing a predetermined calculation operation on a signal added to a command signal transmitted from the interrogator in order to request the transponder to permit communication and for adding a resulting signal to a response signal that is transmitted back to the interrogator; and

an authentication circuit for checking whether the interrogator is authentic or not on a basis of the signal added to the command signal transmitted from the

interrogator in order to request the transponder to permit communication,

wherein the signal obtained through the predetermined calculation operation performed by the calculation circuit so as to be added to the response signal is used as a signal on a basis of which the interrogator checks whether the transponder is authentic or not.

9. A non-contact communications system, comprising:

a plurality of interrogators that are managed by different parties; and

a transponder for data communication having a plurality of storage areas for storing data used when the transponder communicates individually with the interrogators and a plurality of key signals, unique to the transponder and stored one for each of the storage areas, for permitting use of only a particular storage area corresponding to an interrogator with which the transponder is currently communicating,

wherein the transponder, when communicating with an interrogator on a non-contact basis, checks a key signal received from the interrogator against the key signals stored in the transponder and, when the received key signal coincides with one of the stored key signals, the transponder is permitted to communicate with the interrogator by using only a particular storage area corresponding to that interrogator.

10. A non-contact communications system as claimed in claim 9,

wherein the transponder further has an authentication circuit for generating

a signal that is transmitted to the interrogator in order to request the interrogator to permit communication.

11. A non-contact communications system as claimed in claim 9,

wherein the transponder further has an authentication circuit for detecting a signal that is transmitted from the interrogator in order to request the transponder to permit communication, for checking whether the interrogator is authentic or not on a basis of the detected signal, and for permitting communication if the interrogator is found to be authentic.

12. A non-contact communications system as claimed in claim 9,

wherein the transponder further has:

a calculation circuit for performing a predetermined calculation operation on a signal added to a command signal transmitted from the interrogator in order to request the transponder to permit communication and for adding a resulting signal to a response signal that is transmitted back to the interrogator; and

an authentication circuit for checking whether the interrogator is authentic or not on a basis of the signal added to the command signal transmitted from the interrogator in order to request the transponder to permit communication,

wherein the signal obtained through the predetermined calculation operation performed by the calculation circuit so as to be added to the response signal is used as a signal on a basis of which the interrogator checks whether the transponder is authentic or not.

13. A non-contact communications system as claimed in claim 9, wherein, in the transponder, at least one of the storage areas is composed of a count storage member in which a count is stored that is updated in response to a count updating command transmitted from the interrogator when the transponder communicates with the interrogator by using that storage area.

The Patent Office

INVESTOR IN PEOPLE

32

Application No: GB 0004575.7
Claims searched: 1-13

Examiner: Robert Macdonald
Date of search: 31 August 2000

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.R): H4L(LASS, LAX, LADTA, LADTX, LADCS, LADX, LECCP, LECCX)

Int Cl (Ed.7): G06F(12/08); G06K(19/07, 19/077); G07F(7/10); H04L(9/08, 9/12, 9/14, 9/32)

Other: ONLINE: WPI, PAJ, EPODOC

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	EP 0743622 A2	(TOSHIBA) See whole document	1 and 9, at least.
X	EP 0332117 A2	(TOSHIBA) See whole document	1 and 9, at least.
	US 6058477	(SONY) See whole document	
A	US 4734568	(TOPPAN) See whole document.	
X	JP 100327142	(SONY) See enclosed abstract and English language equivalent US 6058477.	1 and 9, at least.

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.